ESD-TR-69-153

# Technical Note 1969-23

B. E. White

# On a Class of Orthogonal Sequences

4 June 1969

Prepared under Electronic Systems Division Contract AF 19(628)-5167 by

Lincoln Laboratory
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Lexington, Massachusetts

The work reported in this document was performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology. The work was sponsored by the U.S. Navy under Air Force Contract AF 19(628)-5167.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

LINCOLN LABORATORY

# ON A CLASS OF ORTHOGONAL SEQUENCES

*B. E. WHITE*

*Group 66*

TECHNICAL NOTE 1969-23

4 JUNE 1969

This document has been approved for public release and sale; its distribution is unlimited.

LEXINGTON MASSACHUSETTS

# ABSTRACT

A cross correlation between two sequences U and V of length n is defined as

$$U \circ V = \frac{1}{n} \sum_{i=1}^{n} (-1)^{p_{i-1}} u_i \circ v_i \; ; \; u \circ v = \begin{cases} 0, & u \neq v \\ 1, & u = v \end{cases}$$

$$p_i = \text{remainder} \left[ \frac{\sum_{j=1}^{i} u_j + v_j}{2} \right] \; ; \; p_0 = 0,$$

where the elements u, v of the sequences are selected from the alphabet 0, 1, 2, . . . , N-1. Investigated are sets of mutually orthogonal sequences, i.e., $\mathcal{O}$ is such a set iff

$$U \circ V = 0, \forall U, V \in \mathcal{O} \ni U \neq V,$$

given N and n. Of interest is the maximal number of sequences in $\mathcal{O}$ and the construction of the canonic form of $\mathcal{O}$ representative of all possible equivalent solutions. This class of orthogonal sequences has application in continuous-phase frequency shift keyed communication, where the N possible frequencies are equally spaced by any odd number of half cycles per signalling interval T, and the duration of the mutually orthogonal waveforms is nT.

In the binary case (N = 2) a one-one, onto linear transformation between n orthogonal sequences of length n in $\mathcal{O}$ and an n × n Hadamard matrix is exhibited. Canonic forms for $\mathcal{O}$'s of maximum size are found for n odd, twice an odd integer, and a power of two. In these instances the maximum number of sequences in $\mathcal{O}$ is two, two, and n, respectively; the number of sequences in $\mathcal{O}$ cannot exceed the length of the sequences for any n that is a multiple of four.

In the general case (N > 2) results are less extensive, especially for N odd. A useful construction technique is given for obtaining an $\mathcal{O}$ of rm sequences of length n in $rN_1$ elements from a smaller orthogonal set of m sequences of length n in $N_1$ elements. For $N_1 = 2$ and m = n it is shown that this construction yields the canonic form of the $\mathcal{O}$ matrix of maximum size.

Accepted for the Air Force
Franklin C. Hudson
Chief, Lincoln Laboratory Office

# CONTENTS

## SYMBOLS

| | |
|---|---|
| $\oplus$ | addition modulo N |
| $+$ | arithmetic addition |
| $\oplus\sum$ | summation modulo N |
| $\sum$ | arithmetic summation |
| $\circ$ | correlation operation |
| $\bullet$ | dot product operation |
| $\times$ | -by- ; arithmetic multiplication |
| $\in$, $\notin$ | is a member of, is not a member of |
| $\ni$ | such that |
| $\exists$, $\nexists$ | there exists, there exists no |
| $\forall$ | for all |
| $\Leftrightarrow$ , iff ; $\Rightarrow$ | if and only if ; implies that |
| $\perp$, $\not\perp$ | is orthogonal to, is not orthogonal to |
| $\{\ \}$ | set |
| $\subset$ | is subset of |
| $\cup$ | union (of sets) |
| $\mathfrak{H}$ | Hadamard matrix composed of the elements 0 and 1 with all 0's in the first row and last column |
| $\mathfrak{H}'$ | $\mathfrak{H}$ with 0 and 1 replaced by 1 and -1, respectively |
| $\mathfrak{J}$ | set of N integer elements 0, 1, 2, . . . N-1 |
| k, $\ell$, m, r, s | positive integers |
| $\mathfrak{m}$ | arbitrary set or matrix of sequences of length n composed from $\mathfrak{J}$ |
| n | sequence length; number of columns in matrix |
| N | number of mutually orthogonal elements |
| $\mathfrak{O}$ | orthogonal set or matrix of sequences in $\mathfrak{S}$ |
| $\mathfrak{O}^t$, $\mathfrak{H}^t$ | transpose of $\mathfrak{O}$, $\mathfrak{H}$ |
| $p_i$ | parity between two sequences following the $i^{th}$ element of each |

| | |
|---|---|
| $\mathfrak{S}$ | set of all possible sequences of length $n$ composed from $\mathcal{J}$ |
| $\mathfrak{T}$ | $n \times n$ matrix composed from $\mathcal{J}$ |
| $\mathfrak{T}^{-1}$ | inverse of $\mathfrak{T}$ |
| $U, V, W, X, Y$ | sequences of length $n$ composed from $\mathcal{J}$ |
| $\overline{U}$ | additive inverse sequence, i.e., $U \oplus \overline{U} = \underline{0} = 0^n$ |
| $\underline{0}$ | identity sequence of all zeros, i.e., $U \oplus \underline{0} = U$ |
| $0^k$, $1^k$ | sequence of $k$ consecutive 0's, 1's |

# I. INTRODUCTION

This work was motivated by studies proposing the use of binary continuous-phase frequency-shift-keying (FSK) (with a frequency spacing of 1/2T, where T is the signalling interval corresponding to one data bit)* for high-power low-frequency communications in military applications. Of interest here are mutually orthogonal N-ary continuous-phase FSK waveforms composed from mutually orthogonal signals equally spaced in frequency by any odd number of half cycles per signalling interval T.

Waveforms are represented by sequences of integers corresponding to the subscripts of the N possible frequencies

$$f_i = f_0 + i\,\Delta f;\ \ 0 \le i \le N-1,$$

where $2T\Delta f$ is an odd positive integer. Signals of duration T at frequencies $f_j$ and $f_i (i \neq j)$ are orthogonal; $2T(f_j - f_i) = 2T\Delta f(j-i) = \left\{\begin{matrix}\text{even}\\ \text{odd}\end{matrix}\right\}$ integer if j and i have $\left\{\begin{matrix}\text{the same}\\ \text{different}\end{matrix}\right\}$ parity. Consequently, the contribution to the cross correlation of two distinct continuous-phase waveforms in a given signalling interval is 0 if $f_j \neq f_i$ or $\left\{\begin{matrix}+1\\ -1\end{matrix}\right\}$ if $f_j = f_i$ and the phase difference is an $\left\{\begin{matrix}\text{even}\\ \text{odd}\end{matrix}\right\}$ multiple of $\pi$ radians at the beginning of the interval.

Given N and a fixed sequence length, the problem is to construct the maximal number of mutually orthogonal sequences, preferably in a canonic form representative of all possible equivalent solutions. The problem is complicated by the three-valued contributions to the cross correlation of sequences; more commonly such contributions are only two-valued as in FSK with a frequency spacing of an integral number of cycles per signalling

* This form of modulation is sometimes referred to as MSK for minimum-shift-keying. The term MSK is usually associated with a particular modem where the data sequence and the frequencies of the transmitted waveform do not directly correspond bit-by-bit (as in the more common FSK modem) but according to a reversible transformation [Ref. 0].

interval. However, the task of finding a set of binary ($N = 2$) orthogonal sequences under the three-valued rule is actually no more difficult than that under the two-valued rule because there exists a linear invertible transformation between the two sets of sequences; much is already known about constructing binary orthogonal sequences under the two-valued rule.

Being inherently a simpler problem which can be treated more thoroughly than the general case, the binary case is emphasized; the $N = 2$ case is of greater practical interest anyway. By dealing principally with the three-valued correlation rule for $N = 2$, it is hoped that some additional insight can be gained for extending the results for $N > 2$ and solving more general problems.

## II. DEFINITIONS

Let the integers $\mathcal{I} = \{0, 1, 2, \ldots, N-1\}$ represent $N$ mutually orthogonal elements, i.e.,

$$u \circ v = \begin{cases} 0, & u \neq v \\ 1, & u = v \end{cases} \quad \forall u, v \in \mathcal{I}, \tag{1}$$

where $\circ$ is a commutative correlation operation. Addition of two n-tuples $U$, $V$ is performed modulo $N$ element-by-element, i.e.,

$$U \oplus V = (u_1 \oplus v_1)(u_2 \oplus v_2) \ldots (u_i \oplus v_i) \ldots (u_n \oplus v_n), \tag{2a}$$

$$\text{where } u_i \oplus v_i = \text{remainder} \left[ \frac{u_i + v_i}{N} \right] \in \mathcal{I} \, \forall u_i, v_i \in \mathcal{I}. \tag{2b}$$

If $\mathcal{S}$ is the set of all possible sequences of the same length composed from $\mathcal{I}$,

$$\exists \, \overline{U} \in \mathcal{S} \ni U \oplus \overline{U} = \underline{0}, \forall U \in \mathcal{S}, \tag{3}$$

where $\overline{U}$ is the additive inverse sequence and $\underline{0} = 00\ldots0$ is the identity sequence under $\oplus$. Obviously, the rules of commutivity, associativity and closure apply in $\mathcal{S}$ under $\oplus$.

The normalized cross correlation of two sequences in $\mathcal{S}$ is defined as

$$U \circ V = \frac{1}{n} \sum_{i=1}^{n} (-1)^{p_{i-1}} u_i \circ v_i, \tag{4a}$$

where the parity between sequences is

$$p_i = \text{remainder} \left[ \frac{\sum_{j=1}^{i} u_j + v_j}{2} \right] \text{ if } p_0 = 0^{*}; \tag{4b}$$

[*] Unless otherwise stated this initial parity is implicitly assumed for every pair of sequences.

depending on the initial conditions, $p_0$ may equal 1 in which case the parity $p_i$ is changed. From (1) and (4), U and V are

$$\left\{\begin{array}{l} \text{identical} \\ \text{orthogonal} \\ \text{antipodal} \end{array}\right\} \Leftrightarrow \quad U \circ V = \left\{\begin{array}{r} 1 \\ 0 \\ -1 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{c} U = V \\ U \perp V \\ U = V \end{array}\right\} \text{ and } p_0 = \left\{\begin{array}{c} 0 \\ 0 \text{ or } 1. \\ 1 \end{array}\right\} \qquad (5)$$

<u>Example</u>: $N = 4,\ n = 8,\ p_0 = 0$

$$\begin{array}{rcl} U & = & 2\ 1\ 3\ 3\ 0\ 3\ 1\ 2 \\ V & = & 0\ 3\ 3\ 2\ 0\ 1\ 1\ 0 \\ \hline U \circ V & = & \frac{1}{8}(0+0+1+0-1+0-1+0) \ = \ -\frac{1}{8}\ . \end{array}$$

A set $\mathcal{O} \subset \mathcal{S}$ of <u>mutually orthogonal sequences</u> is defined as

$$U \circ V = 0, \forall U, V \in \mathcal{O} \ni U \neq V. \qquad (6a)$$

A <u>biorthogonal</u> set $\mathcal{B}$ is defined as

$$U \circ V = \left\{\begin{array}{c} 0 \\ \\ -1 \end{array}\right\} \text{ for } \left\{\begin{array}{l} \text{all but} \\ \\ \text{exactly} \end{array}\right\} \text{ one } V \in \mathcal{B} \ni V \neq U, \qquad (6b)$$

given any $U \in \mathcal{B}$. For any $\mathcal{O}$, a $\mathcal{B}$ can be formed as

$$\mathcal{B} = \mathcal{O} \cup \mathcal{O}', \qquad (6c)$$

where the prime is used to indicate that $p_0 = 0$ for both sequences in $\mathcal{O}$ or both in $\mathcal{O}'$, but $p_0 = 1$ for one sequence from $\mathcal{O}$ and one from $\mathcal{O}'$; except for these initial parities $\mathcal{O}$ and $\mathcal{O}'$ are identical. From (5) and (6a) it is easily verified that (6c) satisfies (6b). This implies that if biorthogonal sequences are of interest, one loses nothing by focusing attention only on orthogonal sequences.

Any set of m distinct sequences of length n in $\mathcal{S}$ can be expressed as an $m \times n$ matrix with each row consisting of one of the sequences in the set.

The matrix is in standard form iff the digital numbers of radix N specified by the rows are in increasing order from top to bottom. Two matrices are equivalent iff they have the same number of rows and columns and the set $\{U \circ V\}$ of numbers resulting from all $\binom{m}{2}$ possible cross correlations between distinct rows in one matrix is identical to that of the other. Because $U \circ V = V \circ U$, any row permutation of a given matrix yields an equivalent matrix, i.e., every matrix is equivalent to its standard form. Since the sign of each term in (4a) depends on the parity between sequences, a column permutation of a given matrix does not necessarily yield an equivalent matrix.

All possible equivalent but distinct matrices can be represented by a single canonic form as defined conceptually by the following algorithm. Put all the matrices in standard form. Set $r = 1$. Compute the arithmetic sum of the digital numbers of radix N specified by the first r rows (numbering from the top) of each matrix under consideration. Eliminate from further consideration all matrices yielding sums which exceed the minimum sum computed for the first r rows. If only one matrix remains, it is the canonic form. If more than one matrix remains, r is increased by one and the summing and elimination operations are repeated. This process obviously terminates with a single remaining matrix before r exceeds the total number of rows in the matrices since no two matrices are identical.

An orthogonal matrix $\mathcal{O}$, representing a set of mutually orthogonal sequences $\{U\}$, is saturated iff no new row, corresponding to a sequence $V \in \mathcal{S}$, can be added to $\mathcal{O}$ without destroying mutual orthogonality, i.e., $\mathcal{O}$ is saturated iff $\nexists V \in \mathcal{S} \ni V \perp U, \forall U \in \mathcal{O}$. Furthermore, $\mathcal{O}$ is maximal iff there exists no orthogonal matrix with more rows than $\mathcal{O}$, but with the same number of columns and the same value of N, of course. A maximal $\mathcal{O}$ is obviously saturated but a saturated $\mathcal{O}$ is not necessarily maximal. The latter statement can be verified by examining all possibilities given the following canonic forms for $N = 4$ and $n = 5$:

$$\mathcal{O} = \underset{\text{saturated}}{\begin{bmatrix} 0&0&0&0&0 \\ 0&0&1&0&0 \\ 1&1&2&1&1 \\ 1&1&3&1&1 \end{bmatrix}} \quad ; \quad \mathcal{O} = \underset{\text{maximal}}{\begin{bmatrix} 0&0&0&0&0 \\ 0&0&1&0&0 \\ 1&1&2&1&1 \\ 1&2&2&2&2 \\ 2&1&3&1&3 \\ 3&2&3&2&3 \end{bmatrix}} \, .$$

## III. SOME USEFUL PROPERTIES

Lemma 1. For $N$ even, $(U \oplus W) \circ (V \oplus W) = U \circ V, \forall U, V, W \in \mathcal{S}$.

Proof: From (1) and the fact that

$$u_i \oplus w_i = v_i \oplus w_i \Leftrightarrow u_i = v_i, \forall u_i, v_i, w_i \in \mathcal{J},$$

$$(u_i \oplus w_i) \circ (v_i \oplus w_i) = u_i \circ v_i, \forall i, \tag{7a}$$

where $W$ is a sequence in $\mathcal{S}$. Referring to (4), for $N$ even

$$(u_j \oplus w_j) + (v_j \oplus w_j) \text{ is } \begin{Bmatrix}\text{even}\\ \text{odd}\end{Bmatrix} \Leftrightarrow u_j + v_j \text{ is } \begin{Bmatrix}\text{even}\\ \text{odd}\end{Bmatrix}, \tag{7b}$$

so $p_i$ is also unchanged by the addition of $W$. For $N$ odd, (7b) holds iff

$$u_j + w_j \text{ and } v_j + w_j \text{ are both} \geq N \text{ or both} < N; \tag{7c}$$

(7a) and (7c) imply $(U \oplus W) \circ (V \oplus W) = U \circ V$, but the latter does not necessarily imply (7c).

Theorem 1. For $N$ even, the identity sequence $\underline{0}$ comprises the first (top) row of canonic form of any matrix.

Proof: If a given matrix $\mathfrak{m} \subset \mathcal{S}$ has an all zero row, the first row of the canonic form of $\mathfrak{m}$ is $\underline{0}$, regardless of whether $N$ is even or odd, from the definition of the canonic form. If $\mathfrak{m}$ has no all zero row, an equivalent matrix with an all zero row can always be obtained for $N$ even by adding the inverse sequence $\overline{U}$ to all rows of $\mathfrak{m}$, where $U$ is any row of $\mathfrak{m}$, i.e., by Lemma 1 and (3), for any fixed $U \in \mathfrak{m}$,

$$\{V \circ W\} = \{(V \oplus \overline{U}) \circ (W \oplus \overline{U})\}, \forall V, W \in \mathfrak{m}$$

and $U \oplus \overline{U} = \underline{0}$ is the row in the equivalent matrix which replaces $U \in \mathfrak{m}$.

A simple counter example for $N = 3$, namely $\mathfrak{m} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \end{bmatrix}$ with cross correlations $\left\{-\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right\}$ shows that the first row of the canonic form of any matrix is not necessarily $\underline{0}$ for N odd. In this case $\mathfrak{m}$ is the canonic form; it is impossible to construct an equivalent matrix with a 00 row.

Theorem 1 permits the simplification of proofs requiring the special treatment of the identity sequence $\underline{0}$. The proofs of some theorems that follow become tedious if the membership of $\underline{0}$ is unspecified. Therefore, in the sequel it is always assumed that $\underline{0}$ is included in the set of sequences of interest for N even.

Lemma 2. If $N = 2$, $\overline{U} = U$ and $U \oplus U = \underline{0}$.

Proof: From (2a) and (3),

$$U \oplus \overline{U} = (u_1 \oplus \overline{u}_1)(u_2 \oplus \overline{u}_2) \ldots (u_i \oplus \overline{u}_i) \ldots (u_n \oplus \overline{u}_n) = \underline{0},$$

which for $N = 2$ can hold iff $\overline{u}_i = u_i$ from (2b).

Theorem 2. If $N = 2$ and $\underline{0} \in \mathfrak{m} \subset \mathfrak{S}$, then $\mathfrak{m}$ is closed only if m is a power of two, where m is the number of sequences in $\mathfrak{m}$.

Proof: For m = 1 and 2, $\mathfrak{m}$ is closed since $\underline{0} \oplus \underline{0} = \underline{0}$ and $\underline{0} \oplus U = U$, where $\{\underline{0}\} = \mathfrak{m}$ for $m = 1$ and $\{\underline{0}, U\} = \mathfrak{m}$ for $m = 2$. Given $U \oplus V \in \mathfrak{m}$, $\forall U, V \in \mathfrak{m}$, $m = 2^r$ and $W \notin \mathfrak{m}$,

$$\forall U \neq \underline{0},\ U \oplus W \neq W \text{ or } V \neq U.$$

Obviously, $U \oplus W = W$ iff $U = \underline{0}$. Suppose $U \oplus W = V$. Then from Lemma 2 and (2),

$$U \oplus W \oplus W \oplus V = V \oplus W \oplus V$$

$$U \oplus \underline{0} \oplus V = W \oplus \underline{0}$$

$$U \oplus V = W,$$

but this contradicts the fact $W \notin \mathfrak{m}$ so $U \oplus W \neq V$. For closure the number of sequences must double by augmenting the sequences generated by $\{U \oplus W\}$

because $U \oplus W = V \oplus W$ iff $U = V$. The proof is completed by induction on the integer $r$.

Theorem 3. If $N = 2$, $\underline{0} \in \mathfrak{G}$, $\mathfrak{G}$ is closed and $\exists W \notin \mathfrak{G} \ni W \perp U$, $\forall U \in \mathfrak{G}$, then $\{U \oplus W\}$ can augment $\mathfrak{G}$ to yield a closed orthogonal matrix with $2m$ rows, where $m$ (a power of two) is the number of rows in $\mathfrak{G}$.

Proof: Everything but the orthogonality properties follow directly from the proof of Theorem 2. Given $W \notin \mathfrak{G} \ni W \circ U = 0, \forall U \in \mathfrak{G}$, by Lemmas 1 and 2 and (2),

$$(U \oplus W) \circ V = (U \oplus W \oplus U) \circ (V \oplus U) = (U \oplus W \oplus \overline{U}) \circ (V \oplus U)$$

$$= (\underline{0} \oplus W) \circ (U \oplus V) = W \circ (U \oplus V) = 0$$

since $U \oplus V \in \mathfrak{G}$, where $U \neq V \in \mathfrak{G}$. By Lemma 1 $(U \oplus W) \circ (V \oplus W) = U \circ V = 0$, $\forall U \neq V$ since $U \perp V$. Finally, by Lemmas 1 and 2 and (2),

$$(U \oplus W) \circ U = (U \oplus W \oplus U) \circ (U \oplus U) = (U \oplus W \oplus \overline{U}) \circ (U \oplus \overline{U})$$

$$= (\underline{0} \oplus W) \circ \underline{0} = W \circ \underline{0} = 0$$

because $W \perp \underline{0}$.

Simple counter examples for $N > 2$ showing that $\mathfrak{m}$ can be closed when $m$ is not a power of two are:

$$\underset{N = 3}{\mathfrak{m} = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}} \quad ; \qquad \underset{N = 4}{\mathfrak{m} = \begin{bmatrix} 00 \\ 12 \\ 32 \end{bmatrix}} \; .$$

The $N = 3$ example, being an orthogonal matrix, shows that a closed $\mathfrak{G}$ with a-power-of-two rows does not necessarily result from every augmentation for $N$ odd.

Corollary 1. If $N = 2$, $\underline{0}$, $\underline{1} \in \mathfrak{G}$ and $\mathfrak{G}$ is closed, then $U \oplus \underline{1} \in \mathfrak{G}$ $\forall U \in \mathfrak{G}$, where $\underline{1} = 11\ldots1$ and $U \oplus \underline{1}$ is the complement of $U$ (for $N = 2$ only).

Proof: This follows directly from Theorem 3. Using Lemmas 1 and 2, verification is straightforward:

$$(U \oplus \underline{1}) \circ U = \underline{1} \circ \underline{0} = 0$$

$$(U \oplus \underline{1}) \circ V = \underline{1} \circ (U \oplus V) = 0, \quad U \neq V \in \mathcal{G}.$$

Lemma 3. The total number of agreements element-by-element between every pair of sequences in $\mathcal{G}$ must be even for any value of N.

Proof: Given any N, from (1), (4a) consists of a normalized arithmetic sum of + 1's and - 1's resulting from agreements between the $i^{th}$ elements of the two sequences involved; disagreements between corresponding elements affect parity but contribute nothing to the summation. Clearly, the sum can be zero only if the total number of + 1's and - 1's is even. However, an even number of agreements does not necessarily imply orthogonality.

## IV. PRINCIPAL RESULTS (BINARY CASE)

### A. Relationship to Hadamard Matrices

Let the normalized dot product of two sequences $X, Y \in \mathcal{S}$ be defined as

$$X \bullet Y = \frac{1}{n} \sum_{i=1}^{n} x_i \circ y_i , \tag{8}$$

where $x_i$ and $y_i$ are the $i^{th}$ elements (from $\mathcal{J}$) of X and Y, respectively[*], and the o operation is defined by (1). Obviously, from (1) and (8), X and Y are

$$\left\{\begin{matrix}\text{identical}\\ \text{orthogonal}\end{matrix}\right\} \Leftrightarrow X \bullet Y = \left\{\begin{matrix}1\\ 0\end{matrix}\right\} \Leftrightarrow \left\{\begin{matrix}X = Y\\ X \perp Y\end{matrix}\right\} \Leftrightarrow \left\{\begin{matrix}x_i = y_i\\ x_i \neq y_i\end{matrix}\right\} \forall i; \tag{9}$$

the orthogonal concept of (9) should not be confused with that of (5). A set $\mathcal{M} \subset \mathcal{S}$ of mutually orthogonal sequences under $\bullet$ is defined as

$$X \bullet Y = 0, \forall X, Y \in \mathcal{M} \ni X \neq Y^{\dagger} \tag{10}$$

in a fashion similar to (6a). Since $X \bullet Y \geq 0$, a biorthogonal set under $\bullet$ over $\mathcal{J}$ in the sense of (6b) does not exist.

A Hadamard matrix $\mathcal{H}$, when represented by an n x n array of 0's and 1's, is a special binary case of (8), where if sequences are identified with the rows of $\mathcal{H}$, then

$$X \bullet Y = \frac{1}{2}, \forall X, Y \in \mathcal{H} \ni X \neq Y; \quad N = 2, \text{ n even}, \tag{11}$$

i.e., every pair of binary sequences in $\mathcal{H}$ agree (disagree) element-by-element in exactly half the columns. A Hadamard matrix is usually presented (without loss of generality) with the first row and column composed entirely of the same symbol; it is assumed that this symbol is 0 for $\mathcal{H}$.

[*] The X, Y (rather than U, V) notation is used to distinguish sequences in $\mathcal{S}$ to which the dot product operation is applied.

[†] (10) is not invoked in this report but is merely noted for completeness.

If a Hadamard matrix $\mathfrak{H}'$ is represented with the symbols 1 and - 1 rather than 0 and 1, it is seen that the sequences in $\mathfrak{H}'$ can be viewed as n mutually orthogonal vectors in an n-dimensional space. This follows because agreements (disagreements) contribute exactly n/2 1's (- 1's) to the dot product

$$X' \bullet Y' = \frac{1}{n} \sum_{i=1}^{n} x_i' y_i' ; \; x_i, y_i \in \{1, -1\},$$

i.e., $$X' \bullet Y' = 0, \forall X', Y' \in \mathfrak{H}' \ni X' \neq Y',$$

and the vectors of $\mathfrak{H}'$ span the n-dimensional space.

A biorthogonal set of 2n sequences of length n composed from the symbols 1 and - 1 can be constructed from every Hadamard matrix by augmenting $\mathfrak{H}'$ with $\overline{\mathfrak{H}'}$, a set of sequences identical to those in $\mathfrak{H}'$ except that 1 and - 1 are interchanged everywhere. This corresponds to (6c) and the set $\mathfrak{H} \cup \overline{\mathfrak{H}}$, where $\overline{\mathfrak{H}}$ is identical to $\mathfrak{H}$ except that 0 and 1 are interchanged everywhere.

Except for n = 2, n must be a multiple of four for any $\mathfrak{H}$. It has been conjectured (but not yet proven or disproven) that $\mathfrak{H}$'s exist for all values of n = 4k; $\mathfrak{H}$'s have been found for all such n less than n = 188[Ref. 1] and many larger values. Methods of constructing $\mathfrak{H}$'s have been studied extensively [Ref. 2]. For this reason a reversible transformation between $\mathfrak{C}$ for N = 2 and $\mathfrak{H}$ could be quite useful, and indeed, it is possible to find such a relationship.

Let $\mathfrak{T}$ be an n X n matrix with elements from $\mathfrak{J}$, and let sequences in $\mathfrak{S}$ be represented as n X 1 (column) matrices, where matrix multiplication is accomplished by the usual rule but over a finite field (a commutative ring with a finite number of elements, a cancellation law and a multiplicative inverse). The linear transformation

$$\mathfrak{T}\, U] = X] \; ; \; \mathfrak{T}\, V] = Y] \qquad (12a)$$

is invertible (one-one, onto) iff the determinant of $\mathfrak{T}$, namely $|\mathfrak{T}|$, is non-zero, i.e., the linear transformation

$$U] = \mathfrak{T}^{-1} X] \; ; \; V] = \mathfrak{T}^{-1} Y] \qquad (12b)$$

$$\Updownarrow$$

$$|\mathfrak{T}| \neq 0 \; ; \; \mathfrak{T}^{-1}\mathfrak{T} = \mathfrak{T}\mathfrak{T}^{-1} = U,$$

where the inverse matrix $\mathfrak{T}^{-1}$ is the transpose of the cofactor matrix (adjoint) of $\mathfrak{T}$ divided by $|\mathfrak{T}|$ and U is the n × n unit matrix (1's on the principal diagonal and 0's elsewhere) [Refs. 3 and 4].

Lemma 4. If N = 2 and n is even, $\exists$ an n × n linear invertible transformation, namely,

$$\mathfrak{T} = \begin{bmatrix} 1 & & & \text{\Large 1} \\ & 1 & & \\ & & \cdot & \\ & & & \cdot \\ \text{\Large 0} & & & \cdot \\ & & & & 1 \end{bmatrix} \text{ with an inverse } \mathfrak{T}^{-1} = \begin{bmatrix} 1 & 1 & & & \text{\Large 0} \\ & 1 & 1 & & \\ & & \cdot & \cdot & \\ & & & \cdot & \cdot \\ & & & & \cdot & \cdot \\ \text{\Large 0} & & & & 1 & 1 \\ & & & & & 1 \end{bmatrix}$$

on sequences in $S \ni \circledcirc$ and $\{X, Y\} \ni X \bullet Y = 1/2, \forall X \neq Y$ are one-one, onto, where it is assumed that all sequences in $\{X, Y\}$ begin with the same element.

Proof: It is easily verified that $|\mathfrak{T}| = |\mathfrak{T}^{-1}| = 1$, so $\mathfrak{T}$ and $\mathfrak{T}^{-1}$ are both linear invertible transformations, i.e., from (12), $\{U\}$ and $\{X\}$ ($\{V\}$ and $\{Y\}$) are one-one, onto. For N = 2, in (8)

$$x_i \circ y_i = x_i \oplus y_i \oplus 1, \text{ from (1)}$$

$$= \oplus\sum_{j=i}^{n} u_j \oplus \oplus\sum_{j=i}^{n} v_j \oplus 1, \text{ from (12a) and } \mathfrak{T}$$

$$= \oplus\sum_{j=i}^{n}(u_j \oplus v_j) \oplus 1 = \oplus\sum_{j=1}^{n}(u_j \oplus v_j) \oplus \oplus\sum_{j=1}^{i-1}(u_j \oplus v_j) \oplus 1$$

$$= p_n \ominus p_{i-1} \oplus 1, \text{ from (4b).}$$

Given $\mathfrak{G}$, the number of agreements when the parity between sequences $p$ is zero must equal that when $p = 1, \forall U, V \in \mathfrak{G} \ni U \neq V$ to satisfy orthogonality. From (4b), $p_0 = 0$ and for $N = 2$, $p$ changes iff there is a disagreement between elements. Assuming that $n$ is even, from Lemma 3 the number of disagreements is even. Therefore, $p_n = 0$ and $x_1 = y_1$, and $p_{i-1}$ and $x_i \circ y_i$ are both $0(1)$ exactly $n/2$ times over the range of $i$. Thus, from (8)

$$X \bullet Y = \frac{1}{2}, \forall X \neq Y,$$

and $\mathfrak{G}$ is transformed one-to-one into the desired $\{X, Y\}$.

Conversely, for $N = 2$, in (4a)

$$u_i \circ v_i = u_i \oplus v_i \oplus 1, \text{ from (1)}$$

$$= \begin{cases} x_i \oplus x_{i+1} \oplus y_i \oplus y_{i+1} \oplus 1;\ i < n \\ \\ x_i \oplus y_i \oplus 1;\ i = n \end{cases} \quad \text{, from (12b) and } \mathfrak{J}^{-1}$$

$$= \begin{cases} p_{i-1} \oplus p_i \oplus 1;\ i < n \\ \\ p_n \oplus p_{i-1} \oplus 1;\ i = n \end{cases} \quad \text{, since } x_i \oplus y_i = p_n \oplus p_{i-1}$$

$$= p_{i-1} \oplus p_i \oplus 1.$$

Given $\{X, Y\} \ni X \bullet Y = 1/2, \forall X \neq Y$ and the fact that $x_i \oplus y_i = p_n \oplus p_{i-1}$, since $p_n$ is fixed and the number of agreements (disagreements) between X and Y must be exactly $n/2$, $p_{i-1} = 0(1)$ exactly half the time, as has already been seen. Assuming $x_1 = y_1$ and that $n$ is even, $p_n = p_0$ and $p_i = 0(1)$ exactly half the time. Therefore, from (4a)

$$U \circ V = \frac{1}{n} \sum_{i=1}^{n} (-1)^{p_{i-1}} (p_{i-1} \oplus p_i \oplus 1)$$

$$= \frac{1}{n} \sum_{i=1}^{n} (1 - p_{i-1} - p_i), \text{ from a truth table}$$

$$= \frac{1}{n} (n - \frac{n}{2} - \frac{n}{2}) = 0,$$

and the specified $\{X, Y\}$ is transposed one-to-one into $\mathfrak{O}$.

Lemma 5. If $N = 2$ and $n$ is even, there exists no $\mathfrak{O}$ containing more than $n$ sequences, where $n$ is the sequence length.

Proof: An $\mathfrak{O}$ with more than $n$ sequences exists iff a corresponding $\{X, Y\} \ni X \bullet Y = \frac{1}{2}$ for $X \neq Y$ exists by Lemma 4. But since a Hadamard matrix $\mathfrak{H}$ of $n$ sequences of length $n$ (see (11)) corresponds to a set of $n$ vectors, namely, those of $\mathfrak{H}'$, that span an n-dimensional space, the specified $\{X, Y\}$ with more than $n$ sequences cannot exist.

## B. Size of Orthogonal Matrices

Theorem 4. If $N = 2$ and $n$ is odd, then the canonic form of the maximal $\mathfrak{O}$ matrix is

$$\begin{bmatrix} & 0^n & \\ 0^{\frac{n-1}{2}} & 1 & 0^{\frac{n-1}{2}} \end{bmatrix},$$

where $n$ is the number of columns in $\mathfrak{O}$ and $0^k$ represents a sequence of $k$ consecutive repetitions of the element 0.

Proof: From Theorem 1 the first row of $\mathfrak{O}$ is $0^n$. Suppose the maximal $\mathfrak{O}$ matrix consists of at least three rows for $N = 2$ and $n$ odd. Then from Lemma 3 the number of agreements between any pair from the first row and any two other given rows of $\mathfrak{S}$ must be even. It is readily verified that this is impossible for n odd. Obviously, the sequence $\perp$ to $\underline{0}$ and specifying the smallest binary number is that represented by the second row in the above matrix. The contribution of the first $(n-1)/2$ columns to the cross correlation is cancelled by that of the last $(n-1)/2$ columns from (4), since the parity changes only at column $(n+1)/2$.

Corollary 2. If $N = 2$ there exists exactly one $\mathfrak{S}$, namely, the trivial set $\begin{bmatrix}0\\1\end{bmatrix}$, where the number of rows exceeds the number of columns in the matrix.

Proof: This follows directly from Theorem 4 for $n = 1$ and Lemma 5.

Theorem 5. If $N = 2$ and n is twice an odd integer, then the canonic form of the maximal $\mathfrak{S}$ matrix is

$$\begin{bmatrix} 0^n \\ 0^{\frac{n}{2}-1}\;1\;0^{\frac{n}{2}-1}\;1 \end{bmatrix}.$$

Proof: From Theorem 1 the first row of $\mathfrak{S}$ is $0^n$. From Lemma 4 an $\mathfrak{S}$ with $n = 2(2^r+1)$ exists iff a corresponding $\mathfrak{H}$ exists. As already mentioned $\mathfrak{H}$'s may exist only for $n = 2$ or $n = 4k$. Therefore, $r = 0$ and $n = 2$ are the only possible values for $\mathfrak{S}$. Obviously, the sequence $\perp$ to $\underline{0}$ above specifies the smallest possible binary number for the canonic form. The contribution of columns 1 through $n/2 - 1$ to the cross correlation is cancelled by that of columns $n/2 + 1$ through $n - 1$.

Theorem 6. If $N = 2$, $n = 4k$ and $\exists$ an $n \times n$ Hadamard matrix $\mathfrak{H}$, then a maximal $\mathfrak{S}$ of n sequences of length n can be found once $\mathfrak{H}$ is known.

Proof: Given an $n \times n$ $\mathfrak{H}$ matrix, an $n \times n$ $\mathfrak{S}$ matrix can be obtained by applying the inverse transformation $\mathfrak{T}^{-1}$ of Lemma 4 to sequences in $\mathfrak{H}$:

$$\mathfrak{S}^t = \mathfrak{T}^{-1}\mathfrak{H}^t,$$

where $\mathfrak{G}^t$ and $\mathfrak{H}^t$ is the transpose matrix of $\mathfrak{G}$ and $\mathfrak{H}$, respectively. By Lemma 5, $\mathfrak{G}$ is maximal. Although the first row of the $\mathfrak{G}$ matrix is all zeros iff that of $\mathfrak{H}$ is all zeros, the resulting $\mathfrak{G}$ matrix is not necessarily in its canonic form.

## V. CONSTRUCTION OF ORTHOGONAL MATRICES

### A. A Binary Construction

Theorem 7. If $N = 2$ and $n = 4k = (2r+1)2^m$, then $\exists$a method of constructing a closed saturated $\mathcal{G}$ of $2^m$ sequences of length $n$ with the canonic form specified by

$$U_1 = 0^n \; ; \; \mathcal{L}_1 = \emptyset \text{, the empty set}$$

$$U_2 = \left[0^{\frac{n}{2}-1} \; 1\right]^2 \; ; \; \ell = 0$$

$$U_{2^{\ell}+1} = \left[0^{n2^{-\ell-1}-1} \; 1 \; 0^{n2^{-\ell-1}}\right]^{2^{\ell}} \; ; \; \ell \geq 1$$

$$U_j = U_1 \oplus \oplus\sum_{\ell \in \mathcal{L}_j} U_{2^{\ell}+1}; \; 1 \leq j \leq 2^m; \; 0 \leq \ell < m,$$

where $U_j$ is the $j^{th}$ row of the matrix $\mathcal{G}$, $U_1$ and $\{U_{2^{\ell}+1}\}$ are the key rows in terms of which any row can be expressed uniquely, $\mathcal{L}_j$ is the set of $\ell$'s corresponding to the places where 1's occur in the binary equivalent of the decimal number $j-1$, i.e.,

$$j-1 = \sum_{\ell \in \mathcal{L}_j} 2^{\ell},$$

and $[\quad]^{exp}$ means that the subsequence bracketed is repeated exp times.

Proof: From the fundamental theorem of arithmetic, any nonzero integer can be expressed as a product of primes that is unique except for the order in which the prime factors occur. Since the only even prime is two and because odd x odd = odd, any $n$ can be expressed as an odd integer $(2r+1)$ times a power of two $(2^m)$. Only $n = 4k$ is of concern here since other values of $n$ are treated by Theorems 4 and 5.

From Theorem 1 the first row of the canonic form is

$$U_1 = 0^n ;$$

the second row is obviously the same as that of Theorem 5, namely

$$U_2 = 0^{\frac{n}{2}-1} 1\, 0^{\frac{n}{2}-1} 1 ;$$

the $U_3$ specifying the smallest possible binary number for the third row is found as follows.

Let $C_{ijL}$ and $C_{ijR}$ represent the cross correlation between rows i and j in columns 1 through n/2 and columns n/2 + 1 through n, respectively, i.e., over the left (L) and right (R) halves of the sequences. For mutual orthogonality,

$$C_{13L} + C_{13R} = C_{23L} + C_{23R} = 0. \tag{13}$$

Since the left half of row 1(2) is identical to the right half, it seems reasonable to attempt a solution with the left half of row 3 being identical to the right half. This along with (13) implies that if the number of ones in either half of row 3 is

$$\left\{\begin{matrix} \text{even} \\ \\ \text{odd} \end{matrix}\right\}, \text{ then } \left\{\begin{matrix} C_{13L} = C_{13R} \\ \\ C_{23L} = C_{23R} \end{matrix}\right\} = 0. \qquad \begin{matrix} (14a) \\ \\ (14b) \end{matrix}$$

For the even (odd) case of (14a) ((14b)), the smallest binary number for the left half of row 3 is $0^{\frac{n}{4}-1} 1\, 0^{\frac{n}{4}-1} 1$ $(0^{\frac{n}{4}-1} 1\, 0^{\frac{n}{4}})$. Choosing the smaller of these alternatives yields

$$U_3 = \left[0^{\frac{n}{4}-1} 1\, 0^{\frac{n}{4}}\right]^2 .$$

The situation now fits that of Theorem 3 with the closed $\mathcal{C}$ (including $\underline{0}$) identified with $\{U_1, U_2\}$ and with $W = U_3$. Thus, $\mathcal{C}$ can be augmented with $U_3$ and $U_2 \oplus U_3$ to yield a closed orthogonal matrix of four rows consisting of $U_1$, $U_2$, $U_3$ and

$$U_4 = U_2 \oplus U_3 = \left[ 0^{\frac{n}{4}-1} \; 1 \right]^4 .$$

Note that $U_1$, $U_2$ and $U_3$ are key rows as defined in Theorem 7, and that $U_4$, being the first non-key row, can be expressed in terms of nonzero [since $\underline{0} \oplus U = U$, $U_1 = 0^n$ need appear explicitly only as the first row] key rows. It can be verified that $\mathcal{L}_1 = \phi$, $\mathcal{L}_2 = \{0\}$, $\mathcal{L}_3 = \{1\}$ and $\mathcal{L}_4 = \{0, 1\}$, according to the definition of $\mathcal{L}_j$ in Theorem 7.

If $k = 1$, $(m = 2,\ r = 0)$ the canonic form of the maximal (by Lemma 5) $\mathcal{C}$ containing four sequences of length four is now constructed:

$$\mathcal{C} = \begin{bmatrix} U_1 \\ U_2 \\ U_3 \\ U_4 \end{bmatrix} = \begin{bmatrix} 0\,0\,0\,0 \\ 0\,1\,0\,1 \\ 1\,0\,1\,0 \\ 1\,1\,1\,1 \end{bmatrix}.$$

If $k > 1$, the question is can any new rows be added without destroying mutual orthogonality?

If $m > 2$, at least four new rows can be added as follows. Assume that the new key row $U_5$ can be composed of four identical subsequences of length $n/4$ and still be $\perp$ to $U_1$, $U_2$, $U_3$ and $U_4$. It follows that $U_5$ must have an even number of ones in the first $n/2$ columns. From reasoning similar to that which led to $U_3$, it is seen that $C_{15L} = C_{45L} = 0$ must hold. Thus, the problem is reduced to finding the left half of $U_5$ specifying the smallest binary number that is $\perp$ to both the left halves of $U_1$ and $U_4$:

$$
\begin{aligned}
U_{1L} &= 0^{\frac{n}{2}} \\
U_{4L} &= \left[0^{\frac{n}{4}-1}\ 1\right]^2 .
\end{aligned}
$$

But this is equivalent to finding $U_3$ given $U_1$ and $U_2$, so

$$
U_5 = \left[0^{\frac{n}{8}-1}\ 1\ 0^{\frac{n}{8}}\right]^4 .
$$

It is easily verified that $U_5 \perp U_2, U_3$.

Using Theorem 3 the following additional rows are generated:

$$
\begin{aligned}
U_6 &= U_2 \oplus U_5 = \left[0^{\frac{n}{8}-1}\ 1\ 0^{\frac{n}{4}-1}\ 1\ 0^{\frac{n}{8}-1}\ 1\right]^2 \\
U_7 &= U_3 \oplus U_5 = \left[0^{\frac{n}{8}-1}\ 1\ 0^{\frac{n}{8}-1}\ 1\ 0^{\frac{n}{8}-1}\ 1\ 0^{\frac{n}{8}}\right]^2 \\
U_8 &= U_4 \oplus U_5 = U_2 \oplus U_3 \oplus U_5 = \left[0^{\frac{n}{8}-1}\ 1\right]^8 .
\end{aligned}
$$

According to the definition of $\mathcal{L}_j$, $\mathcal{L}_5 = \{2\}$, $\mathcal{L}_6 = \{0, 2\}$, $\mathcal{L}_7 = \{1, 2\}$ and $\mathcal{L}_8 = \{0, 1, 2\}$.

If $k = 2$ $(m = 3,\ r = 0)$ the canonic form of the maximal (by Lemma 5) $\mathfrak{S}$ containing eight sequences of length eight is now constructed:

$$
\mathfrak{S} = \begin{bmatrix} U_1 \\ U_2 \\ U_3 \\ U_4 \\ U_5 \\ U_6 \\ U_7 \\ U_8 \end{bmatrix} = \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0\,1\,0\,0 \\ 0\,1\,0\,1\,0\,1\,0\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0 \\ 1\,0\,1\,1\,1\,0\,1\,1 \\ 1\,1\,1\,0\,1\,1\,1\,0 \\ 1\,1\,1\,1\,1\,1\,1\,1 \end{bmatrix} .
$$

If $k > 2$ and $m > 3$, it is now shown by induction that the number of rows can continue to be doubled using new key rows until $2^m$ rows are constructed.

Suppose that the canonic form of a closed $\mathcal{C}$ with $4 \le 2^{\ell} < 2^m$ rows and the structure specified in Theorem 7 has been found. Assume that a new key row $U_{2^{\ell}+1}$ can be composed of $2^{\ell}$ identical subsequences of length $n2^{-\ell}$ and still be $\perp$ to every row of $\mathcal{C}$. From the key row structure and the definition of $\mathcal{L}_j$, it can be seen that

$$U_{2^{\ell}} = \left[0^{n2^{-\ell}-1}1\right]^{2^{\ell}} . \tag{15}$$

Regardless of whether the number of ones in the $U_{2^{\ell}+1}$ subsequence is odd or even, $U_{2^{\ell}+1}$ must be $\perp$ to both $U_1$ and $U_{2^{\ell}}$ over the first $n2^{-\ell+1}$ columns. This follows because the number of ones in both $U_{2^{\ell}}$ and $U_{2^{\ell}+1}$ is even over these columns, so $U_1 \circ U_{2^{\ell}+1}$ and $U_{2^{\ell}} \circ U_{2^{\ell}+1}$ are both $2^{\ell-1}$ times the respective cross correlations over these columns. Thus, the problem is reduced to finding the subsequence of $U_{2^{\ell}+1}$ specifying the smallest binary number $\perp$ to both the subsequences

$$0^{n2^{-\ell+1}}$$

$$0^{n2^{-\ell}-1}1\,0^{n2^{-\ell}-1}1.$$

But since $n2^{-\ell}-1$ is an odd integer, this is equivalent to finding $U_3$ given $U_1$ and $U_2$, so

$$U_{2^{\ell}+1} = \left[0^{n2^{-\ell-1}-1}1\,0^{n2^{-\ell-1}}\right]^{2^{\ell}} \tag{16}$$

is the appropriate new key row for the canonic form. The next step is to verify that $U_{2^{\ell}+1}$ is $\perp$ to all rows of $\mathcal{C}$.

From the structure of $\mathcal{C}$, for every $1 \le j \le 2^{\ell}$, $U_j$ can have ones only in columns $sn2^{-\ell}$, where $1 \le s \le 2^{\ell}$, and the left half of $U_j$ must be repeated. From (16), $U_{2^{\ell}+1}$ has zeros in columns $sn2^{-\ell}$ and an odd number (precisely one) of ones in the bracketed subsequence. Let $\eta$ be the number of ones in the left half of $U_j$. If $\eta$ is odd, $U_{2^\ell+1} \perp U_j$ since $U_{2^\ell+1} \circ U_j$ over the first n/2 columns is cancelled by that over the last n/2 columns, the relevant parities being $p_0 = 0$ and $p_{n/2} = 1$. The $\eta = 0$ case implying $U_j = U_1$ is already accounted for: $U_{2^\ell+1} \perp U_1$ by construction. If $\eta \neq 0$ is even, let $s_i$ be the value of s locating the $i^{th}$ one in $U_j$. If $s_1$ is even, it can be verified that $U_{2^\ell+1} \circ U_j$ over columns $\left\{\begin{matrix} 1 \text{ through } s_1 n2^{-\ell} \\ s_1 n2^{-\ell}+1 \text{ through } \frac{n}{2} \end{matrix}\right\}$ is cancelled by that over columns $\left\{\begin{matrix} \frac{n}{2}+1 \text{ through } \frac{n}{2}+s_1 n2^{-\ell} \\ \frac{n}{2}+s_1 n2^{-\ell}+1 \text{ through } n \end{matrix}\right\}$, since the number of intervening ones is odd.

Is $s_1$ is odd, a closer examination reveals that $U_{2^\ell+1} \circ U_j$ over columns 1 through $s_1 n2^{-\ell}$ and $n/2+1$ through $n/2+s_1 n2^{-\ell}$ is zero. Proceeding to the right, if $s_2$ is even, the contributions of columns $s_1 n2^{-\ell}+1$ through $s_2 n2^{-\ell}$ and $n/2+s_1 n2^{-\ell}+1$ through $n/2+s_2 n2^{-\ell}$ are also zero. This leaves an even number of ones remaining in the left halves of both $U_{2^\ell+1}$ and $U_j$. Hence, the situation is equivalent to that at the beginning with $\eta$ even; the portions of $U_{2^\ell+1} \circ U_j$, unaccounted for are reduced, however, so a continuation of this process leads to an end. If $s_2$ is odd, the contributions of columns $s_1 n2^{-\ell}+1$ through $(s_1+1)n2^{-\ell}-1$ and $n/2+s_1 n2^{-\ell}+1$ through $n/2+(s_1+1)n2^{-\ell}-1$ are zero, and $U_{2^\ell+1} \circ U_j$ over columns

$\left\{\begin{matrix} (s_1+1)n2^{-\ell} \text{ through } s_2 n2^{-\ell} \\ s_2 n2^{-\ell}+1 \text{ through } \frac{n}{2} \end{matrix}\right\}$ is cancelled by that over columns

$\left\{\begin{matrix} \frac{n}{2}+(s_1+1)n2^{-\ell} \text{ through } \frac{n}{2}+s_2 n2^{-\ell} \\ \frac{n}{2}+s_2 n2^{-\ell}+1 \text{ through } n \end{matrix}\right\}$.

since the number of intervening ones is odd. Thus, $U_{2^\ell+1} \perp U_j, \forall 1 \leq j \leq 2^\ell$.

Using Theorem 3 a new closed orthogonal matrix of $2^{\ell+1}$ rows in canonic form is obtained by augmenting $\mathfrak{C}$ with the $2^\ell$ sequences $\{U_{2^\ell+1} \oplus U_j\}$. When $2^m$ rows are generated, the number of consecutive zeros

$$n2^{-m}-1 = (2r+1)2^{m-m}-1 = 2r$$

at the beginning of rows $2^{m-1}+1$ through $2^m$ is an even integer, and a new key row of the form of (16) no longer exists.

It is now shown that no new row can augment the constructed $\mathfrak{C}$ of $2^m$ rows without destroying mutual orthogonality. It is easily shown (by setting $r = 0$) that $\mathfrak{C}$ consists of the maximal canonic orthogonal matrix $\mathfrak{C}_m$ for sequences of length $2^m$ with 2r columns of all zeros before each column of $\mathfrak{C}_m$. By Lemma 4, $\mathfrak{C}_m$ corresponds to a $2^m \times 2^m$ Hadamard matrix $\mathfrak{H}_m$. If the $n \times n$ transformation $\mathfrak{J}$ of Lemma 4 is applied to the transpose matrix $\mathfrak{C}^t$,

$$\mathfrak{J}\mathfrak{C}^t = \mathfrak{H}^t_{me},$$

it is seen that the effect of the all zero columns of $\mathfrak{C}$ is to expand $\mathfrak{H}_m$ by repeating each element of $\mathfrak{H}_m$ 2r times to form the expanded Hadamard matrix $\mathfrak{H}_{me}$. As an example, consider the $\mathfrak{C}$ constructed for $n = 12$:

$$\mathfrak{C} = \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1 \\ 0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1 \end{bmatrix}; \quad \mathfrak{C}_m = \begin{bmatrix} 0\,0\,0\,0 \\ 0\,1\,0\,1 \\ 1\,0\,1\,0 \\ 1\,1\,1\,1 \end{bmatrix};$$

$$\mathfrak{H}_{me} = \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1 \end{bmatrix}; \quad \mathfrak{H}_m = \begin{bmatrix} 0\,0\,0\,0 \\ 0\,0\,1\,1 \\ 0\,1\,1\,0 \\ 0\,1\,0\,1 \end{bmatrix}.$$

From (11) and the fact that $\mathcal{H}_{me}$ is an expanded Hadamard matrix, the dot product of every pair of sequences in $\mathcal{H}_{me}$ is 1/2. If a new row X can augment $\mathcal{H}_{me}$ while preserving dot products of 1/2, then using Lemma 4 the new row $\mathcal{J}^{-1}X]$ can augment $\mathcal{G}$ without destroying mutual orthogonality. Let $a_i$ $(2r+1-a_i)$ be the number of zeros (ones) in the $i^{th}$ $(1 \le i \le 2^m)$ subsequence of length $2r+1$ in X. Then it is possible to write the set of linear equations

$$\mathcal{H}'_m \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_i \\ \cdot \\ \cdot \\ \cdot \\ a_{2^m} \end{bmatrix} = \begin{bmatrix} n/2 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} ,$$

as can be seen from the $n = 12$ example:

$$a_1 + a_2 + a_3 + a_4 = 6$$

$$a_1 + (3-a_2) + (3-a_3) + a_4 = 6$$

$$(3-a_1) + (3-a_2) + a_3 + a_4 = 6$$

$$(3-a_1) + a_2 + (3-a_3) + a_4 = 6.$$

Since $\mathcal{H}'_m$ represents a set of $2^m$ linearly independent vectors (composed of 1's and -1's) which span a $2^m$ dimensional space, the vector $\mathcal{A} = a_1a_2 \ldots a_i \ldots a_{2^m}$ can be expressed as a linear combination of the vectors of $\mathcal{H}'_m$. Since $\mathcal{A}$ is parallel to the first row vector $1^{2^m}$ of $\mathcal{H}'_m$ and $\perp$ to all the other vectors of $\mathcal{H}'_m$, all the a's must be equal. But since

$$\sum_{i=1}^{2^m} a_i = \frac{n}{2}$$

must hold, and because $2r+1$ is odd, integer solutions for the a's are impossible:

$$2^m a_i = \frac{n}{2} \Rightarrow a_i = n2^{-m-1} = \frac{2r+1}{2} .$$

Therefore, $\mathcal{C}$ cannot be augmented by any row and is saturated by the $2^m$ rows of the construction. This finally completes the proof of Theorem 7.

Corollary 3. If $N = 2$ and $n = 2^m (m \geq 2)$, the construction of Theorem 7 results in the canonic form of the closed maximal $\mathcal{C}$ of $2^m$ rows.

Proof: This follows directly from Theorem 7 for $r = 0$ and Lemma 5.

Corollary 4. If $N = 2$, $n = 4k = (2r+1)2^m$ and $r \neq 0$, the construction of Theorem 7 cannot result in a maximal $\mathcal{C}$ if an $n \times n$ Hadamard matrix exists.

Proof: This follows directly from Theorems 6 and 7; $n = 12$ is the smallest possible example of a maximal, but not necessarily canonic and not closed (see Theorem 2), $\mathcal{C}$ which cannot be obtained by Theorem 7:

$$\mathcal{C} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&0&0&0&0&1 \\ 0&0&1&0&1&1&0&0&1&0&1&1 \\ 0&1&0&0&0&1&0&1&0&1&0&0 \\ 0&1&0&1&1&0&0&1&0&1&1&0 \\ 0&1&1&1&1&1&1&0&1&0&0&1 \\ 1&0&0&1&0&0&0&1&1&1&0&1 \\ 1&0&1&0&0&1&0&0&0&1&0&0 \\ 1&0&1&1&0&1&1&1&0&0&1&1 \\ 1&1&0&1&0&0&1&1&1&1&1&0 \\ 1&1&1&0&1&0&1&1&1&0&1&0 \\ 1&1&1&1&1&0&1&0&1&1&1&1 \end{bmatrix} .$$

Corollary 5. If $N = 2$ and $n = 2^m (m \geq 1)$, rows $U_j$ and $U_{n-j+1}$ are complementary, i.e., $U_j \oplus U_{n-j+1} = 1^n$, in the canonic form of the closed maximal $\mathcal{C}$, where $1 \leq j \leq 2^m$.

Proof: For $m = 1$ this is obvious from Theorem 5. For $m > 1$, from Theorem 7 and (15), if $n = 2^m$, $U_{2^m} = 1^n$. By Corollary 1 and the fact that $\mathfrak{S}$ is closed and in standard form,

$$U_j \oplus U_{n-j+1} = 1^{2^m} \text{ must hold } \forall 1 \le j \le 2^m.$$

B. Some General Results (N-ary Case)

Theorem 8. Given any N and any orthogonal set $\mathfrak{S}_1 \subset \mathcal{S}_1$ consisting of m sequences of length n composed from the elements $\mathcal{J}_1 = \{0, 1, \ldots N_1 - 1\}$, a corresponding orthogonal set

$$\mathfrak{S} = \mathfrak{S}_\Delta \bigcup_{i=1}^{r} \mathfrak{S}_i$$

of $rm + \Delta$ sequences of length n composed from the elements $\mathcal{J} = \{0, 1, \ldots, N-1\}$ can be constructed from $\mathfrak{S}_1$, where $\mathfrak{S}_i$ is obtained by replacing element $0 \le u \le N_1 - 1$ in $\mathfrak{S}_1$ with element $(i-1)N_1+u$, and $\mathfrak{S}_\Delta$ is an orthogonal set of $\Delta$ sequences composed from the left-over elements $\{rN_1, rN_1+1, \ldots, N-1\}$ (if any).

Proof: Obviously, the sequences in $\mathfrak{S}_i$ are $\perp$ to the sequences in $\mathfrak{S}_j$ $(i \ne j)$ and $\mathfrak{S}_\Delta$ since the sets of elements $\{(i-1)N_1+u\}$, $\{(j-1)N_1+u\}$ and $\{rN_1, rN_1+1, \ldots, N-1\}$ are disjoint. Referring to (1) and (4), the sequences of $\mathfrak{S}_i$ are mutually orthogonal because

$$[(i-1)N_1+u] \circ [(i-1)N_1+v] = u \circ v = \begin{cases} 0, & u \ne v \\ 1, & u = v \end{cases};$$

$$\text{remainder}\left[\frac{\sum (i-1)N_1+u+(i-1)N_1+v}{2}\right] = \text{remainder}\left[\frac{\sum u+v}{2}\right].$$

Note that if $\mathfrak{S}_1$ is maximal, $\mathfrak{S}$ is not necessarily maximal. For example, with $N = 4$, $N_1 = 2$, $n = 6$ and

$$\mathfrak{S}_1 = \begin{bmatrix} 0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,1 \end{bmatrix} \quad \text{(see Theorem 5)},$$

Theorem 8 yields

$$\mathfrak{S} = \begin{bmatrix} 0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,1 \\ 2\,2\,2\,2\,2\,2 \\ 2\,2\,3\,2\,2\,3 \end{bmatrix},$$

but the maximal canonic form obtained by an exhaustive technique is

$$\begin{bmatrix} 0&0&0&0&0&0 \\ 0&0&1&0&0&1 \\ 1&1&2&1&1&2 \\ 1&2&2&1&2&2 \\ 2&3&0&2&3&0 \\ 2&3&1&2&3&1 \\ 3&1&3&3&1&3 \\ 3&2&3&3&2&3 \end{bmatrix} .$$

Also, for $N = 3$ and $\Theta_1$ the same as above, $\Theta_\Delta = [222222]$ but the maximal canonic form (again obtained by exhaustion) is

$$\begin{bmatrix} 0&0&0&0&0&0 \\ 0&0&1&2&0&0 \\ 0&1&0&0&1&0 \\ 1&1&2&1&1&1 \\ 1&2&2&1&2&1 \end{bmatrix} .$$

<u>Lemma 6a</u>. Given any $N$ and a binary sequence $B$ of length $n$ composed from the elements $0, 1$, the set $\{U(B)\}$ contains at most

$$\eta = \begin{cases} \left.\begin{matrix} \frac{N}{2} \text{ (N even)} \\ \frac{N-1}{2} \text{ (N odd)} \end{matrix}\right\} B \neq 0^n \\ \\ \left.\begin{matrix} \frac{N}{2} \text{ (N even)} \\ \frac{N+1}{2} \text{ (N odd)} \end{matrix}\right\} B = 0^n \end{cases}$$

mutually orthogonal sequences, where $U(B)$ is defined as any sequence $U \epsilon \mathcal{S}$ which maps into $B$ when the even(odd) elements of $U$ are replaced by $0(1)$.

Proof: Let $b_i$, $u_i$ and $v_i$ be the $i^{th}$ element of $B$, $U(B)$ and $V(B)$, respectively, where $V(B)$ is also a member of $\{U(B)\}$.. By definition

$$b_i = \begin{Bmatrix} 0 \\ 1 \end{Bmatrix} \Leftrightarrow u_i = \begin{Bmatrix} \text{even} \\ \text{odd} \end{Bmatrix} \Leftrightarrow v_i = \begin{Bmatrix} \text{even} \\ \text{odd} \end{Bmatrix},$$

i.e., the $i^{th}$ elements of any two sequences $U(B)$, $V(B) \epsilon \{U(B)\}$ have the same parity, $\forall 1 \leq i \leq n$. From this and (4b) the parity between sequences U(B) and V(B) is $p_i = 0, \forall i$. Hence from (1) and (4a), $U(B) \circ V(B) = 0$ iff $u_i \neq v_i, \forall i$. For N even(odd) there are N/2 (N+1/2) even elements and N/2 (N-1/2) odd elements in $\mathcal{J} = \{0, 1, 2, \ldots, N-1\}$. If $B \neq 0^n$ the number of mutually orthogonal sequences in $\{U(B)\}$ is limited to the number of odd elements in $\mathcal{J}$, namely, N/2 (N-1/2) for N even (odd) since $u_i \neq v_i$ must hold $\forall i$ for $U(B) \perp V(B)$. If $B = 0^n$, U(B) and V(B) consist of only even elements, so the number of mutually orthogonal sequences in $\{U(B)\}$ is limited to the number of even elements in $\mathcal{J}$, namely, N/2 (N+1/2) for N even (odd).

Lemma 6b. Given any N and any two sequences $U_i, U_j \in \mathcal{S}$ specifying $\{U_i(B_i)\}$, $\{U_j(B_j)\} \ni U_i \perp U_j$ but $B_i \not\perp B_j$, at most

$$\eta = \begin{cases} \left.\begin{array}{ll} \frac{N}{2} & (N \text{ even}) \\ \frac{N-1}{2} & (N \text{ odd}) \end{array}\right\} & \text{neither } B_i \text{ nor } B_j = 0^n \\ \left.\begin{array}{ll} \frac{N}{2} & (N \text{ even}) \\ \frac{N+1}{2} & (N \text{ odd}) \end{array}\right\} & \text{either } B_i \text{ or } B_j = 0^n \end{cases}$$

mutually orthogonal sequences can be selected from

$$\{U_i(B_i)\} \cup \{U_j(B_j)\},$$

where B and U(B) are defined in Lemma 6a.

Proof: If $B_i = B_j$, $\{U_i(B_i)\} = \{U_j(B_j)\}$ and everything follows from Lemma 6a. If $B_i \neq B_j$, let

$$U_i = u_{i1} \ldots u_{ik} \ldots u_{in}$$

$$U_j = u_{j1} \ldots u_{jk} \ldots u_{jn},$$

$$B_i = b_{i1} \ldots b_{ik} \ldots b_{in}$$

$$B_j = b_{j1} \ldots b_{jk} \ldots b_{jn} ,$$

$$\{U_i(B_i)\} = \{B_i \oplus 2\alpha\}$$

$$\{U_j(B_j)\} = \{B_j \oplus 2\beta\} ,$$

$$\alpha = \alpha_1 \ldots \alpha_k \ldots \alpha_n$$

$$\beta = \beta_1 \ldots \beta_k \ldots \beta_n , \text{ where}$$

$$\alpha_k, \beta_k = \{0, 1, 2, \ldots, \left\{\begin{array}{ll} \frac{N}{2} - 1 & \left.\begin{array}{l} \text{N even} \\ \text{N odd} \end{array}\right\} b_{ik}, b_{jk} = 0 \\ \frac{N-1}{2} & \\ \frac{N}{2} - 1 & \left.\begin{array}{l} \text{N even} \\ \text{N odd} \end{array}\right\} b_{ik}, b_{jk} = 1. \\ \frac{N-3}{2} & \end{array}\right.$$

In addition, let

$$\mathcal{A} = \{k\} \ni u_{ik} = u_{jk}$$

$$\left\{\begin{array}{c} \mathcal{B} \\ \mathcal{C} \end{array}\right\} = \{k\} \ni u_{ik} \neq u_{jk} \text{ and } u_{ik} + u_{jk} \text{ is } \left\{\begin{array}{c} \text{odd} \\ \text{even} \end{array}\right\} .$$

Suppose a set $\{B_i \oplus 2\alpha_\ell\}$ of $\eta$ mutually orthogonal sequences including $U_i$ is selected, where $\alpha_\ell$ is the specific $\alpha$ determining the $\ell^{\text{th}}$ sequence in the set. Since $\{b_{ik} \oplus 2\alpha_{\ell k}\}$ over $\ell$ is composed of distinct elements, $\forall k$ and because $U_i \circ U_j = 0$, the contribution to $U_j \circ (B_i \oplus 2\alpha_\ell)$ from $\mathcal{A}$ is zero, $\forall \ell$; the contribution from $\beta$ is also zero since $b_{ik} \oplus 2\alpha_{\ell k}$ and $u_{jk}$ have different parities for $\beta$. Because $U_i \circ U_j = 0$ and $B_i \circ B_j \neq 0$, $\mathcal{C}$ is not an empty set, and the number of distinct k's in $\mathcal{C}$ at an even relative phase does not equal that for an odd phase. Thus, since only one of the $\eta$ distinct elements $\{b_{ik} \oplus 2\alpha_{\ell k}\}$ can equal $u_{jk}$ for each value of $k \in \mathcal{C}$, there must be at least one sequence in $\{B_i \oplus 2\alpha_\ell\}$ which is not orthogonal to $U_j$. By similar reasoning it follows that if $\{B_i \oplus 2\alpha_\ell\}$ contains fewer than $\eta$ sequences, at most $\eta$ mutually orthogonal sequences from $\{B_i \oplus 2\alpha\} \cup \{B_j \oplus 2\beta\}$ are possible. Since $\eta$ sequences can be obtained from $\{U_i(B_i)\}$ (see Lemma 6a), nothing is gained by choosing a $U_j \perp U_i$ if $B_j \not\perp B_i$.

Lemma 6c. Given any N and any two sequences $U_i$, $U_j \in \mathcal{S}$ specifying $\{U_i(B_i)\}$, $\{U_j(B_j)\} \ni U_i \perp U_j$ and $B_i \perp B_j$, at most

N (any N) either $B_i$ or $B_j = 0^n$

$$\left.\begin{array}{ll} N & (N \text{ even}) \\ N-1 & (N \text{ odd}) \end{array}\right\} \text{ neither } B_i \text{ nor } B_j = 0^n$$

mutually orthogonal sequences can be selected from

$$\{U_i(B_i)\} \cup \{U_j(B_j)\},$$

where B and U(B) are defined in Lemma 6a.

Proof: Referring to the proof of Lemma 6b for $B_i \neq B_j$, $B_i \circ B_j = 0$ implies that the number of distinct k's in $\mathcal{C}$ at an even relative phase equals that for an odd phase. Hence, since only one element of $\{b_{ik} \oplus 2\alpha_{\ell k}\}$ can equal $u_{jk}$ for each value of $k \in \mathcal{C}$, and because $b_{jk} \oplus 2\beta_{\ell k}$ can assume only distinct values, where $\beta_\ell$ is the specific $\beta$ determining the $\ell^{th}$ sequence of the mutually orthogonal set $\{B_j \oplus 2\beta_\ell\}$ including $U_j$, it is always possible for $(B_i \oplus 2\alpha_\ell) \circ (B_j \oplus 2\beta_m) = 0, \forall \ell, m$. The maximum number of mutually orthogonal sequences selected from $\{B_i \oplus 2\alpha\} \cup \{B_j \oplus 2\beta\}$ is obtained from Lemma 6a by summing over these two disjoint sets.

Lemma 6d. Given any N, at most

$$\left\{\begin{matrix} \frac{nN}{2} \\ \frac{n}{2}(N-1)+1 \end{matrix}\right\} \text{ for } N \left\{\begin{matrix} \text{even} \\ \text{odd} \end{matrix}\right\} \text{ and } n > 1$$

mutually orthogonal sequences from $\mathcal{S}$ can exist.

Proof: The number of binary sequences in the maximal $\mathcal{B}$ is n from Lemma 5 with the exception of the $n = 1$ case (see Corollary 2). From Lemma 6c there can be at most $N/2$ mutually orthogonal sequences for each $B_i$ in $\mathcal{B}$ for N even; for N odd, this number is $(N-1)/2$ for each $B_i \neq 0^n$ in $\mathcal{B}$ and $(N+1)/2$ sequences can be added for $0^n$ in $\mathcal{B}$ (see Lemma 6a).

Theorem 9. Given any N and a binary set $\mathcal{B}_1 \subset \mathcal{S}_1$ of n ($n = 2$ or a multiple of 4) sequences of length n composed from the elements $\mathcal{J}_1 = \{0, 1\}$, the set $\mathcal{B}$ constructed in Theorem 8 with

$$r = \left\{\begin{matrix} \frac{N}{2} \\ \frac{N-1}{2} \end{matrix}\right\} \text{ and } \Delta = \left\{\begin{matrix} 0 \\ 1 \end{matrix}\right\} \text{ for } N \left\{\begin{matrix} \text{even} \\ \text{odd} \end{matrix}\right\}$$

is maximal; if $\mathcal{B}_1$, expressed as a matrix, is in the canonic form, then the matrix $\mathcal{B}$ is also canonic provided $\mathcal{B}_i$ is placed above $\mathcal{B}_{i+1}, \forall 1 \leq i \leq r$, and if (for N odd) $\mathcal{B}_\Delta = (N-1)^n$ constitutes the last row.

Proof: There are

$$rn+\Delta = \left\{\begin{matrix} \frac{n}{2}N \\ \frac{n}{2}(N-1)+1 \end{matrix}\right\}, \quad N \left\{\begin{matrix} \text{even} \\ \text{odd} \end{matrix}\right\}$$

mutually orthogonal sequences in $\mathcal{B}$ from Theorem 8. From Lemma 6d, $\mathcal{B}$ is maximal. If the matrix $\mathcal{B}_1$ is in canonic form, then $\mathcal{B}$ must also be canonic by the construction of Theorem 8, where elements of $\mathcal{J} = \{0, 1, \ldots, N-1\}$ are taken in pairs, namely, $(i-1)2$ and $(i-1)2+1$ to compose $\mathcal{B}_i$, according to increasing values with increasing i. This follows from the definition of the canonic form, Lemma 5 and Lemma 6 which, in effect, preclude the choice of an $\mathfrak{C}_i$ involving elements in addition to or instead of (i-1)2 and (i-1)2+1 if the canonic form is desired. Note that for these elements $\mathfrak{C}_i$ is in canonic form (from Theorem 8).

A simple example of the maximal canonic form of Theorem 9 for N = 6 and n = 4 is

$$\mathfrak{C} = \begin{bmatrix} 0&0&0&0\\ 0&1&0&1\\ 1&0&1&0\\ 1&1&1&1\\ 2&2&2&2\\ 2&3&2&3\\ 3&2&3&2\\ 3&3&3&3\\ 4&4&4&4\\ 4&5&4&5\\ 5&4&5&4\\ 5&5&5&5 \end{bmatrix},$$

where

$$\mathfrak{C}_1 = \begin{bmatrix} 0&0&0&0\\ 0&1&0&1\\ 1&0&1&0\\ 1&1&1&1 \end{bmatrix}$$

is the maximal canonic form for $N_1 = 2$ and $n = 4$ (see Theorem 7). If N = 7, the maximal canonic form is obtained by augmenting the above $\mathfrak{C}$ with a thirteenth row 6666. It is obvious from this example that $\mathfrak{C}$ is not necessarily closed in Theorem 8 even if $\mathfrak{C}_1$ is closed.

## VI. DISCUSSION

Since the basic results of this report are presented as theorems in the text and are summarized in the abstract, they are not repeated here. Instead, several items of interest are mentioned which may be useful in extending these results or that help explain why extensions may be more difficult to obtain.

The integers $\mathcal{J}$ constitute a commutative ring under addition $\oplus$ and multiplication $\otimes$ modulo N; $\mathcal{J}$ is a field iff N is prime. In this report only the operation $\oplus$ is used. A property analogous to Lemma 1 using the operation $\otimes$ exists, however, and is stated without proof: for N even,

$$(U \otimes W) \circ (V \otimes W) = U \circ V, \forall U, V, W \in \mathcal{S}$$

$$\ni w_i \neq 0 \text{ and g.c.d. } (N, w_i) = 1, \forall i.$$

In general, neither this property nor Lemma 1 holds for N odd. Thus, the N odd case can only be more difficult than the N even case.

Lemma 2 can be generalized for N even as

$$U \oplus \overline{U} = \underline{0} \Leftrightarrow u_i = 0 \text{ or } \frac{N}{2}, \forall i,$$

but this property appears to have value only in the binary case. Similarly, the notion of complementation for N even is

$$U \oplus U_{\text{comp}} = \left(\frac{N}{2}\right)^n; \; u_{i\,\text{comp}} \ni u_i \oplus u_{i\,\text{comp}} = \frac{N}{2}, \forall i.$$

The binary case is fundamentally simpler than the general case because N = 2 is the only even prime.

Although the rows of a matrix can be permuted without changing the set of cross correlations between distinct row pairs, this is not generally true under any permutation of the columns since the parities between rows may change (see (4)). The following two column operations are manageable, however.

Let a cyclic shift of $\tau$ be defined as

$$U(\tau) = u_{n-\tau+1} \cdots u_n u_1 \cdots u_{n-\tau} \; ; \; 0 \le \tau \le n,$$

and let $U \circ V|$ and $|U \circ V$ represent the first $n-\tau$ and last $\tau$ terms of (4a), respectively. Then from (4b)

$$U(\tau) \circ V(\tau) = \left\{ \begin{array}{l} |U \circ V, \text{ if } p_0 = p_{n-\tau} \\ -|U \circ V, \text{ if } p_0 \neq p_{n-\tau} \end{array} \right\} + \left\{ \begin{array}{l} U \circ V|, \text{ if } p_{n-\tau} = p_n \\ -U \circ V|, \text{ if } p_{n-\tau} \neq p_n \end{array} \right\} .$$

Similarly, defining a reversal as

$$U' = u_n \cdots u_{n-i+1} \cdots u_1 ; \quad 1 \le i \le n,$$

then

$$U' \circ V' = \left\{ \begin{array}{l} U \circ V, \text{ if } p_0 = p_n \\ -U \circ V, \text{ if } p_0 \neq p_n \end{array} \right. .$$

These properties hold for any N, but seem to have limited value.

The dot product (8) is introduced primarily to exhibit a reversible transformation from binary orthogonal sequences under (4) to sequences of a Hadamard matrix. The transformation preserves mutual orthogonality of sequences under the o operation and the common dot product n/2 of the corresponding sequences under the • operation. An interesting question is whether there exist similar transformations for other values of N, not only for orthogonal sequences but near-orthogonal sequences as well. This could yield results (of the same nature as, but more general than Theorem 6) which facilitate the transfer of information about sequences under the o and • operations.

The binary construction of Theorem 7 has two main features. Most important is the realization of the maximal canonic form of $\mathcal{C}$ for $n = 2^m$ $(m \geq 2)$. If $n = (2r+1)2^m (m \geq 2; r \neq 0)$ the disparity between $2^m$, the number of sequences in the saturated $\mathcal{C}$ obtained by Theorem 7, and n, the number of sequences in the maximal set obtained by Theorem 6, can be quite marked. This suggests that the efficacy of a construction technique depends on n, as is the case with Hadamard matrices. An arbitrary choice of a new sequence orthogonal to a given unsaturated $\mathcal{C}$ (as in Theorem 7) can limit the eventual number of sequences in the saturated set.

In general, Theorem 8 gives only a lower bound to the number of sequences in the maximal $\mathcal{C}$ for $N > 2$ and a means of constructing a set which achieves the lower bound from a smaller known set $(\mathcal{C}_1)$. Theorem 9 indicates that the construction of Theorem 8 results in the maximal (i.e., the upper bound is achieved by the lower bound) canonic matrix $\mathcal{C}$ for any N and $n = 2$ or a multiple of 4 provided the maximal canonic form of the smaller matrix $\mathcal{C}_1$ is known. Since maximal $\mathcal{C}_1$'s are known for many values of n of practical interest, Theorem 9 (along with the construction of Theorem 8) is of fundamental importance in the N-ary case.

# REFERENCES

0. Doelz and Heald, "Minimum-Shift Data Communication System," U. S. Government Patent No. 2,977,417 (28 March 1961).

1. Berlekamp, Algebraic Coding Theory, (McGraw-Hill, 1968).

2. Hall, Combinatorial Theory, (Blaisdell, 1967).

3. Hoffman and Kunze, Linear Algebra, (Prentice-Hall, 1961).

4. Birkhoff and MacLane, A Survey of Modern Algebra, (MacMillan, 1965).

## DOCUMENT CONTROL DATA - R&D

*(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)*

1. ORIGINATING ACTIVITY *(Corporate author)*
Lincoln Laboratory, M.I.T.

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP
None

3. REPORT TITLE
On a Class of Orthogonal Sequences

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*
Technical Note

5. AUTHOR(S) *(Last name, first name, initial)*
White, Brian E.

6. REPORT DATE
4 June 1969

7a. TOTAL NO. OF PAGES
46

7b. NO. OF REFS
5

8a. CONTRACT OR GRANT NO.
AF 19(628)-5167

b. PROJECT NO.
1508A

c.

d.

9a. ORIGINATOR'S REPORT NUMBER(S)
Technical Note 1969-23

9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
ESD-TR-69-153

10. AVAILABILITY/LIMITATION NOTICES
This document has been approved for public release and sale; its distribution is unlimited.

11. SUPPLEMENTARY NOTES
None

12. SPONSORING MILITARY ACTIVITY
U.S. Navy

13. ABSTRACT

A cross correlation between two sequences U and V of length n is defined as

$$U \circ V = \frac{1}{n} \sum_{i=1}^{n} (-1)^{p_{i-1}} u_i \circ v_i \; ; \; u \circ v = \begin{cases} 0, & u \neq v \\ 1, & u = v \end{cases}$$

$$p_i = \text{remainder} \left[ \frac{\sum_{j=1}^{i} u_j + v_j}{2} \right] ; \; p_0 = 0,$$

where the elements u, v of the sequences are selected from the alphabet 0, i, 2, ..., N-1. investigated are sets of mutually orthogonal sequences, i.e., $\mathcal{O}$ is such a set iff

$$U \circ V = 0, \forall U, V \in \mathcal{O} \ni U \neq V,$$

given N and n. Of interest is the maximal number of sequences in $\mathcal{O}$ and the construction of the canonic form of $\mathcal{O}$ representative of all possible equivalent solutions. This class of orthogonal sequences has application in continuous-phase frequency shift keyed communication, where the N possible frequencies are equally spaced by any odd number of half cycles per signalling interval T, and the duration of the mutually orthogonal waveforms is nT.

in the binary case (N = 2) a one-one,. onto linear transformation between n orthogonal sequences of length n in $\mathcal{O}$ and an n × n Hadamard matrix is exhibited. Canonic forms for $\mathcal{O}$'s of maximum size are found for n odd, twice an odd integer, and a power of two. In these instances the maximum number of sequences in $\mathcal{O}$ is two, two, and n, respectively; the number of sequences in $\mathcal{O}$ cannot exceed the length of the sequences for any n that is a multiple of four.

In the general case (N > 2) results are less extensive, especially for N odd. A useful construction technique is given for obtaining an $\mathcal{O}$ of rm sequences of length n in $rN_1$ elements from a smaller orthogonal set of m sequences of length n in $N_1$ elements. For $N_1 = 2$ and m = n it is shown that this construction yields the canonic form of the $\mathcal{O}$ matrix of maximum size.

14. KEY WORDS

orthogonal sequences
FSK communication
waveforms
binary sequences
Hadamard matrix